

Magistrate Judge McCandlis

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

VOLODYMYR KVASHUK,

Defendant.

CASE NO. MJ19-321

COMPLAINT for VIOLATION

Title 18, U.S.C., Section 1341

BEFORE, the Honorable Paula L. McCandlis, United States Magistrate Judge,
U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT 1

(Mail Fraud)

A. Background

1. At all relevant times, Microsoft Corporation ("Microsoft") was an American multinational corporation headquartered in Redmond, Washington, that developed, manufactured, licensed, supported and sold computer software, consumer

1 electronics and personal computers and services. Microsoft maintained an online store
2 that was accessible to the general public via the Internet. A customer looking to purchase
3 products from Microsoft could establish an account (linked to the customer's email
4 address) and purchase various items from Microsoft, including digital currency (such as a
5 digital gift card) that could be redeemed for other Microsoft products or services.

6 2. Microsoft assigned a group of software testers (the "Universal Store Team"
7 or "UST") to make simulated purchases of products from the online store. The purpose
8 of the testing program was to ensure that customers could make purchases smoothly and
9 efficiently. VOLODYMYR KVASHUK was a member of the testing group during the
10 August 2016 to June 2018 timeframe. For part of that time period, VOLODYMYR
11 KVASHUK was employed by an outside vendor that supplied testers to Microsoft. For
12 the remained of that timeframe (except a short period) VOLODYMYR KVASHUK was
13 directly employed by Microsoft.

14 **B. The Scheme To Defraud**

15 3. In order to conduct testing, UST members first had to establish a test
16 customer account with the Microsoft online store. The test store account would be linked
17 to an email account created specifically for the purposes of testing. The test email
18 account would include the tester's name (or some portion of the name). The UST team
19 would then "whitelist" the test store account, meaning that purchases made from the
20 account would automatically bypass Microsoft's security and risk protocols, which
21 monitored online purchases in order to detect possible fraud. The test accounts were
22 linked to artificial payment devices ("Test in Production" or "TIP" cards) – in effect,
23 phony credit cards – that allowed the tester to simulate a purchase without generating an
24 actual charge.

25 4. The testing program was designed to block the delivery of physical goods.
26 Microsoft did not anticipate that testers would make test purchases of digital currency
27 ("Currency Stored Value" or "CSV") and thus no safeguards were put in place to prevent
28

1 the delivery of CSV. Thus, a tester who purchased CSV using a test account would
2 receive valuable CSV that could then be used to purchase Microsoft products or services.

3 5. The essence of the scheme and artifice to defraud was for VOLODYMYR
4 KVASHUK to use his role as a tester of Microsoft's online store to obtain property,
5 including CSV, from Microsoft through materially false and misleading pretenses,
6 representations, and statements. VOLODYMYR KVASHUK resold much of the
7 fraudulently obtained digital currency to third parties. During the course of the scheme,
8 VOLODYMYR KVASHUK fraudulently obtained over \$10,000,000 in CSV and other
9 property from Microsoft. VOLODYMYR KVASHUK knew that he was not authorized
10 to obtain CSV in his role as a tester, and disguised his identity using various false and
11 misleading pretenses, representations, and statements.

12 **C. Manner and Means**

13 6. It was part of the scheme and artifice to defraud that, in 2017, while
14 employed by a Microsoft vendor and assigned to the UST, VOLODYMYR KVASHUK
15 began using the test account created for him (the "vokvas" account) to make
16 unauthorized purchases of CSV from Microsoft's online store. VOLODYMYR
17 KVASHUK purchased over \$10,000 of CSV from approximately April to October of
18 2017.

19 7. It was further part of the scheme and artifice to defraud that
20 VOLODYMYR KVASHUK redeemed some of the CSV he obtained during this period
21 and used it to make purchases. In several instances, VOLODYMYR KVASHUK
22 concealed his identity as the person who was redeeming the CSV by using Microsoft
23 store accounts that were not in his name. In at least one instance, VOLODYMYR
24 KVASHUK redeemed some of the CSV – using it to purchase a subscription to Microsoft
25 Office – via a Microsoft store account established in the name of a business that
26 VOLODYMYR KVASHUK was associated with. In other instances, VOLODYMYR
27 KVASHUK redeemed the CSV using store accounts that were linked to temporary email
28 accounts that did not contain VOLODYMYR KVASHUK's name in the email address,

1 namely pikimajado@tinoza.org (the "pikimajado" account) and xidijenizo@axsup.net
2 (the "xidijenizo" account). Furthermore, VOLODYMYR KVASHUK concealed his
3 connection to the pikimajado and xidijenizo accounts by providing a false name and a
4 false address as contact information for the store accounts.

5 8. It was further part of the scheme and artifice to defraud that, on or about
6 October 22nd and October 24th of 2017, VOLODYMYR KVASHUK used the redeemed
7 funds in the pikimajado and xidijenizo accounts to order three GeForce GTX 1070 video
8 or "graphics" cards with a total cost of approximately \$2,024.58 from Microsoft's online
9 store. The cards were shipped by Federal Express, a private or interstate commercial
10 carrier, from Ontario, California, to Seattle, Washington, on or about October 22nd and
11 October 24th of 2017.

12 9. It was further part of the scheme and artifice to defraud that, beginning in
13 approximately November of 2017, VOLODYMYR KVASHUK escalated the scale of his
14 unauthorized CSV purchases. To conceal his identity, VOLODYMYR KVASHUK
15 avoided using the "vokvas" test account that was associated with himself, and began
16 using test accounts created for, and associated with, other members of the UST, namely
17 the "av," "sf," and "za" accounts. Between approximately November 26, 2017, and
18 March 23, 2018, VOLODYMYR KVASHUK purchased over \$10,000,000 in CSV from
19 these accounts. In addition to using accounts associated with other testers,
20 VOLODYMYR KVASHUK used one or more services specializing in Internet
21 anonymity to conceal his role in the unauthorized purchases of CSV.

22 10. It was further part of the scheme and artifice to defraud that
23 VOLODYMYR KVASHUK used reseller websites to sell at least some of the CSV to
24 third parties, who could then redeem the CSV and purchase items from Microsoft.
25 VOLODYMYR KVASHUK used the proceeds of the scheme to purchase property for
26 his own benefit, including a home and a vehicle.

1 **D. Execution Of The Scheme To Defraud**

2 11. On or about October 22, 2017, at Seattle, within the Western District of
3 Washington and elsewhere, VOLODYMYR KVASHUK, for the purposes of executing
4 the above-described scheme to defraud and to obtain money and property, and attempting
5 to do so, did knowingly cause to be sent and delivered by Federal Express, a private and
6 commercial interstate carrier, one or more Microsoft graphics cards, from Ontario,
7 California, to Seattle, Washington.

8 All in violation of Title 18, United States Code, Section 1341.

9
10 And the complainant states that this Complaint is based on the following
11 information:

12 I, MICHAEL SPIESS, being first duly sworn on oath, depose and say:

13 **Affiant's Background**

14 1. I am a Special Agent with the United States Secret Service ("USSS"), and
15 have been since September 22, 2002. I am currently assigned to the Seattle Field Office.
16 I am a graduate of the Federal Law Enforcement Training Center located in Glynco,
17 Georgia, and the USSS Special Agent Training Program located in Beltsville, Maryland.
18 Before becoming a Special Agent, I was employed with the USSS as a Uniformed
19 Officer in Washington, D.C. Before that, I served as a United States Immigration
20 Inspector in Toronto, Canada. I have a Bachelor of Arts Degree from Daemen College in
21 Amherst, New York. In the course of my official duties as a Special Agent, I have
22 investigated a broad range of financial crimes, including credit card fraud, bank fraud,
23 access device fraud, embezzlement, corporate theft of monies, money laundering, and
24 counterfeit currency and securities. As a result, I have experience with various methods
25 and practices used by criminals to commit fraud.

26 2. For purposes of conducting this investigation and drafting this affidavit, I
27 have spoken to other agents, law enforcement officials and witnesses. The statements
28 contained in this affidavit are based on my personal knowledge, and on information that

1 has been provided to me directly or indirectly by other investigating agents, and on my
2 experience and training. I also have reviewed files and reports provided by other law
3 enforcement agencies and public databases and records. Some of the information in this
4 affidavit was provided to me by Internal Revenue Service Special Agent Eric Hergert.
5 SA Hergert is a member of the investigative team, and is extremely familiar with
6 electronic evidence, cybercrime, and technologies related to computers and the Internet.
7 SA Hergert also has specialized training in cryptocurrencies, with a focus on Bitcoin and
8 Ethereum. This has included training into how publically viewable "blockchains" record
9 cryptocurrency transactions, how to trace funds through these transactions, attribution
10 techniques used to identify individuals responsible for conducting the transactions, and
11 methods used by individuals to obfuscate the source of, or their control of,
12 cryptocurrencies. SA Hergert has used these techniques in prior and ongoing
13 investigations. Additionally, SA Hergert has conducted cryptocurrency training for
14 others, both internal to the IRS, as well as for external third parties.

15 3. This affidavit does not detail each and every fact and circumstance that I or
16 others have learned during the course of this investigation. Rather, this affidavit serves
17 solely to establish that there is probable cause to believe that VOLODYMYR
18 KVASHUK committed the crime of Mail Fraud in violation of Title 18, United States
19 Code, Section 1341.

20 Summary

21 4. VOLODYMYR KVASHUK is a Ukranian citizen who has been living in
22 the United States since 2015. The investigation has shown that KVASHUK devised and
23 executed a scheme to defraud Microsoft Corporation ("Microsoft"). KVASHUK worked
24 for Microsoft and was assigned to test the company's online retail sales platform. In that
25 role, KVASHUK was supposed to make simulated purchases of Microsoft products from
26 the company's online store. The testing system was designed to ensure that no physical
27 products would be shipped. KVASHUK, however, used test accounts to purchase
28 massive amounts of "currency stored value," or "CSV," such as digital gift cards. The

1 testing program was not supposed to involve purchases of CSV, and no mechanisms were
2 in place to prevent the delivery of valuable CSV to the tester. The investigation has
3 shown that KVASHUK, in his role as a tester, purchased millions of dollars of CSV,
4 which he then resold on the Internet. KVASHUK used the proceeds of the fraud to
5 purchase, among other things, a \$160,000 Tesla car and a \$1.6 million home in Renton.

6 The Investigation

7 5. As part of this investigation, I have obtained records from numerous
8 sources, met with counsel for Microsoft, and interviewed Microsoft employees who
9 investigated the CSV theft.

10 Microsoft's Program To Test Online Retail Sales

11 6. Microsoft has given me a copy of VOLODYMYR KVASHUK's resume,
12 which shows that he is a Seattle-based software engineer. According to information
13 provided by Microsoft, KVASHUK was an employee of a Microsoft vendor. As part of
14 his employment with the vendor, KVASHUK worked on matters for Microsoft from
15 August 26, 2016, until October 1, 2017. During that time, KVASHUK worked out of
16 Microsoft's office and had access to the company's computer network. On December 1,
17 2017, Microsoft hired KVASHUK as a full-time employee with an annual salary of
18 approximately \$116,000. KVASHUK worked for Microsoft until June 22, 2018.

19 7. Microsoft sells various products to the general public over the Internet via
20 its online store. To make purchases from the Microsoft store, a customer must establish a
21 Microsoft store account that is linked to an email address and to one or more payment
22 devices (such as a credit card). As both an employee of an outside vendor, and as a
23 Microsoft employee, KVASHUK was a member of Microsoft's Universal Store Team
24 ("UST"), which supports the company's online retail platform by (among other things)
25 managing a program that tests the online sales system.

26 8. The testing program involves creating test Microsoft store accounts that are
27 linked to test email accounts created specifically for the purpose of the testing program.

28 A tester creates a test email account by using a naming convention for the account: the

1 name begins with “mstest,” followed by an underscore and the user name of the tester.
 2 The tester then requests that the UST team “whitelist” the account, meaning that
 3 purchases made from the account will automatically bypass Microsoft’s security and risk
 4 protocols, which monitor online purchases in order to detect possible fraud. The test
 5 accounts are linked to artificial payment devices (“Test in Production” or “TIP” cards) –
 6 in effect, phony credit cards – that allow the tester to simulate a purchase without
 7 generating an actual charge. Once the whitelisted account is created, the tester uses that
 8 account to attempt to make online product purchases from Microsoft, just as an ordinary
 9 consumer would. Although each test account was created for a particular tester, the login
 10 and password information for the test accounts was stored in an electronic document that
 11 was accessible to multiple testers. Microsoft investigators told me that, in practice,
 12 testers sometimes used test accounts set up for other testers.

13 9. According to Microsoft, the testing program was designed to test the
 14 company’s online sales of physical goods only. When a tester used a whitelisted account
 15 to purchase physical goods, the system ensured that no goods were actually delivered.

16 10. According to Microsoft, the testing program was not designed for simulated
 17 purchases of electronic currency stored value (“CSV”), such as digital gift cards. Testers
 18 were not authorized to use test accounts to make test purchases of CSV. Because
 19 Microsoft did not expect testers to purchase CSV, the system had no safeguards to
 20 prevent the delivery of actual, usable CSV to a tester who made a purchase from a
 21 whitelisted account. Accordingly, if a tester did purchase CSV, the system would
 22 generate a valid and usable product “key” that could be “redeemed,” meaning that the
 23 value of the digital currency would be added to an electronic “wallet” linked to a
 24 customer account. Once redeemed, the CSV could be used to buy both physical and
 25 digital products from the Microsoft store.

26 The Theft Of \$10 Million In Microsoft’s Digital Currency

27 11. According to information provided by Microsoft, in February of 2018,
 28 Microsoft’s UST Fraud Investigation Strike Team (“FIST”) noticed a suspicious increase

1 in the use of CSV to buy subscriptions to Microsoft's Xbox live gaming system from
2 Microsoft's online store. FIST investigated and discovered that the suspicious CSV had
3 originally been purchased from Microsoft through two whitelisted test accounts
4 associated with the email accounts I will refer to as the "av" and "sf" accounts. The CSV
5 was then resold on the secondary market, at a steep discount, via at least two online
6 reseller websites, g2a.com and nokeys.com. Customers who purchased the CSV on the
7 secondary market then redeemed the CSV at Microsoft's online store for Xbox live
8 subscriptions.

9 12. The websites g2a.com and nokeys.com are located at IP addresses
10 88.198.39.152 and 67.229.64.252, respectively. According to open source research, the
11 servers hosting these websites are located in Germany and California, respectively.

12 13. The av and sf test accounts were not established by KVASHUK, but rather
13 by other Microsoft employees. However, the username and passwords for those and
14 other test accounts were stored on Microsoft's network, giving KVASHUK and many
15 other Microsoft employees access to them. FIST discovered that the av and sf test
16 accounts were used to buy a large amount of CSV between November 2017 and March
17 2018. The av and sf accounts were blocked by Microsoft on or about March 15, 2018.
18 FIST later discovered that a third test account I will refer to as the "za" account was also
19 responsible for a suspicious spike in CSV purchases, conducting approximately 166
20 purchases of CSV between March 22 and March 23, 2018. This account was blocked on
21 or about March 23, 2019

22 14. The three suspicious test accounts were used to purchase roughly \$10.1
23 million in CSV from Microsoft. Microsoft was able to "blacklist" roughly \$1.8 million in
24 CSV to prevent it from being redeemed, resulting in a total loss to Microsoft of
25 approximately \$8.3 million.

CSV Redemptions by Acquisition Account

Account	2017	2018	Total
av	\$357,595.00	\$1,298,010.00	\$1,655,605.00
sf	\$601,261.27	\$5,444,340.04	\$6,045,601.31
za	\$0.00	\$643,380.00	\$643,380.00
Total	\$958,856.27	\$7,385,730.04	\$8,344,586.31

15. Microsoft interviewed the employees who created the three suspicious test accounts and found no evidence that they were involved in the fraudulent CSV purchases.

Evidence Of Kvashuk's Involvement In The Theft

16. A variety of evidence shows that KVASHUK was involved in the CSV theft from Microsoft.

Kvashuk's Use Of His Own Test Account For Theft

17. As an initial matter, KVASHUK has admitted to Microsoft investigators that he used the Microsoft store test account that he created – linked to mstest_v-vokvas@outlook.com (the “vokvas” test account”) – to make unauthorized purchases. Microsoft records show that the vokvas test account made purchases (typically of CSV) on April 28, July 10, September 29, October 4, October 7, October 11, and October 22 of 2017. The amount of CSV obtained through the vokvas account totaled approximately \$12,304.99, of which approximately \$4,464.99 was redeemed.¹

18. On October 7, 2017, the vokvas test account was used to purchase an electronic “token” for a subscription to Microsoft Office for \$164.99. That token was redeemed by a Microsoft store account linked to the email address admin@searchdom.io. Microsoft records show that the name on the Microsoft online store account for

¹ Approximately \$100 of the redeemed CSV appears to have been in Canadian currency. It was not possible to determine from the records available how much of the \$12,304.99 in CSV obtained through the vokvas account was in a foreign currency.

1 “searchdom” is “Volo kvashuk,” and the address is an apartment complex, 5035 15th
 2 Avenue, Unit 101, in Seattle (the “15th Avenue” apartment). A copy of KVASHUK’s
 3 resume (provided by Microsoft) lists him as the co-founder and Chief Technology Officer
 4 of “SearchDom.” Washington Secretary of State records list KVASHUK as a “governor”
 5 for Searchdom, Inc. Also listed as a “governor” in Secretary of State records is “L.W.”
 6 Additionally, L.W. is the registrant contact for the domain name searchdom.io.
 7 According to records obtained from Namecheap, the domain name was registered in
 8 January 21, 2017.

9 19. According to Microsoft records, KVASHUK’s vokvas test account was
 10 used to purchase approximately \$10,164.99 in CSV in October 2017.

11 20. On October 22 and 24, 2017, approximately \$2,500 in CSV obtained by the
 12 vokvas test account was redeemed to Microsoft store accounts linked to the email
 13 addresses pikimajado@tinoza.org (the “pikimajado” account) and xidijenizo@axsup.net
 14 (the “xidijenizo” account). Subscriber information has not been obtained for these email
 15 addresses. Based on open source research, it appears these email addresses may be
 16 associated with temporary email services. These services often do not log subscriber
 17 information, and only keep the email account active for a few minutes.

18 21. On October 22 and 24, 2017, the redeemed funds in the pikimajado and
 19 xidijenizo accounts were used to order three GeForce GTX 1070 video or “graphics”
 20 cards with a total cost of approximately \$2,024.58 from Microsoft’s online store.²
 21 Microsoft’s records show that the name and address associated with the Microsoft online
 22 store accounts linked to the pikimajado and xidijenizo email accounts is “Grigor shikor”
 23 at the same 15th Avenue apartment complex that KVASHUK lived at, but at Unit 309
 24 (instead of KVASHUK’s unit, 101). Microsoft provided the FedEx tracking numbers for
 25 the shipment of these cards. By entering the tracking numbers into FedEx’s website, I
 26 _____

27 ² Microsoft records show attempts to access the vokvas test account from IP addresses located in Russia and Japan
 28 on October 22, 2017. These may have been attempts by KVASHUK to disguise his IP address, although that has
 not been confirmed.

1 was able to determine that the video cards were shipped from Ontario, California to
2 Seattle, Washington on or about October 22nd and 24th of 2017. Additionally, FedEx's
3 website indicated that at least one of the video cards was delivered to the recipient
4 address.

5 22. From my training and experience, I know that FedEx is a "private or
6 commercial interstate carrier" as that term is used in Title 18, United States Code,
7 Section 1341.

8 23. Public records searches did not identify anyone by the name of "Grigor
9 Shikor" in Washington. However, a Grigoriy Kvashuk was identified as living in
10 Oregon. As part of my investigation, investigators obtained phone records for 951-397-
11 8122, which is listed as KVASHUK's phone on his resume. The subscriber name on that
12 account is "Grigory Kvashuk." Additionally, the Washington Department of Licensing
13 lists KVASHUK and Grigoriy Kvashuk as registered owners of a Honda Insight.

14 24. According to Microsoft records, approximately \$600 of the CSV purchased
15 by the vokvas account was redeemed to a Microsoft store account linked to the email
16 address safirion@outlook.com (the "safirion" account). The registered name associated
17 with the safirion@outlook.com email account is "volo kv". The current address is on 7th
18 Avenue in Seattle, and the former address was KVASHUK's apartment at the 15th
19 Avenue complex.

20 25. Microsoft investigators interviewed KVASHUK on May 10 and May 18 of
21 2018. Although no law enforcement officer was at those interviews, I have listened to
22 recordings of the interviews. The interviews were not completely recorded because of a
23 technical problem, but I have also read summaries of the interviews and spoken with
24 Microsoft investigator Andy Cookson, who was present at both interviews.

25 26. The interviewers asked KVASHUK about the purchases made with the
26 vokvas test account. KVASHUK admitted that he had created the vokvas account. He
27 also admitted to making some unauthorized purchases from the account. KVASHUK
28 suggested that there was a lack of guidance from his superiors about what could and

1 could not be purchased via a test account, and claimed to have only been told that test
 2 accounts should not be used to purchase subscriptions.³ KVASHUK claimed that he
 3 believed it was permissible to use test accounts to buy CSV because it was not “real”
 4 money.

5 27. KVASHUK admitted to Microsoft investigators that he used his test
 6 account to purchase CSV. He admitted that the “safirion” account was his personal
 7 account, and that he used stolen CSV to buy movies from the Microsoft store.
 8 KVASHUK admitted that he had tried to buy a video card, but claimed that it had never
 9 arrived.

10 28. The investigators asked KVASHUK about the video cards purchased (using
 11 CSV obtained by the vokvas test account) in the name of “Grigor Shikor” at Unit 309 of
 12 the 15th Avenue complex. KVASHUK denied purchasing those cards. When asked if he
 13 knew “Grigor Shikor,” KVASHUK initially said, “it’s complicated,” but then denied
 14 knowing him.⁴ KVASHUK admitted that he lived at the 15th Avenue complex, but
 15 denied receiving the cards.

16 29. With respect to the Office subscription purchased by the searchdom
 17 account (using a token obtained by the vokvas test account), KVASHUK said that he and
 18 another person were business partners in SearchDom. KVASHUK said that he did not
 19 remember this event and suggested that he might have made a mistake.

20 30. According to Microsoft records, prior to November 22, 2017, all of the
 21 CSV acquired through the vokvas account was redeemed to Microsoft online store
 22 accounts associated with the email addresses admin@searchdom.io,
 23 xidijenizo@axsup.net, or pikimajado@tinzoa.org.

24 31. According to records obtained from Google, on November 22, 2017, at
 25 approximately 12:17 PM, KVASHUK conducted an internet search for “cash in xbox
 26 _____

27 ³ Microsoft investigators have stated that the testers may not have been specifically told that purchasing CSV was
 28 prohibited, as the possibility that testers would purchase CSV was simply not contemplated.

⁴ This part of the interview was not recorded.

1 gift.” Then KVASHUK immediately visited the website, gameflip.com. Gameflip.com
 2 advertises that it allows users to list Xbox Live gift cards for sale on its site. After a gift
 3 card is purchased by a customer, Gameflip.com deposits the proceeds into the seller’s
 4 “gameflip wallet.” The seller can then withdraw the proceeds “any time into your
 5 PayPal, bank account, or Bitcoin.”

6 32. Subsequently, on November 22, 2017, at approximately 7:48 PM, \$50
 7 Canadian of CSV acquired through the vokvas account was redeemed to an unknown
 8 individual’s Microsoft store account associated with the email address
 9 sunmoon94@hotmail.ca. Over the next few days, approximately 12 more redemptions of
 10 CSV acquired by the vokvas account (totaling approximately \$1,150 (\$50 of which was
 11 Canadian)) were made to Microsoft store accounts associated with email addresses with
 12 no known connection to KVASHUK. Based on this information, it appears he began
 13 selling the CSV through third party websites on or about November 22, 2017.

14 *Evidence Linking KVASHUK to CSV Thefts Through Other Test Accounts.*

15 33. The vast majority of the \$10 million in stolen CSV was obtained through
 16 the av, sf, and za test accounts. As noted, although these accounts were created by other
 17 testers, KVASHUK would have had access to the login information necessary to access
 18 these accounts. Furthermore, Microsoft investigators stated that – by using test accounts
 19 set up for other testers, rather than this own test account – KVASHUK made it more
 20 difficult for Microsoft to identify him as a suspect in the thefts.⁵ Based on information
 21 provided by Microsoft, it appears that these accounts were used to make unauthorized
 22 CSV purchases from approximately November 26, 2017, through March 23, 2018.⁶ As
 23 best as can be determined from the available information, it appears that CSV was resold
 24
 25

26
 27 ⁵ As previously noted, Microsoft investigators also told me that the test accounts were sometimes shared among
 testers who were using the accounts for legitimate testing.

28 ⁶ KVASHUK was not employed at Microsoft for the early part of this time period, but could have used any Internet-
 enabled device to access and log into the test accounts.

1 (most likely at a steep discount) through online resellers to customers who used the CSV
2 to make purchases from Microsoft's online store.

3 34. Although KVASHUK admitted to only making very limited purchases of
4 CSV from his test account, the investigation has shown probable cause to believe that
5 KVASHUK used the av, sf, and za accounts to make unauthorized CSV purchases.
6 Some of the evidence comes in the form of Internet Protocol ("IP") address data. An IP
7 address is a numerical label assigned to each device that is connected to a computer
8 network that accesses the Internet. In general, Microsoft's online sales platform records
9 the IP addresses used to access the company's website. However, because the test
10 accounts bypassed several safeguards, IP addresses were only captured on approximately
11 489 of 1,554 transactions.

12 35. Microsoft records show that between December 29, 2017, and March 23,
13 2018, at least \$2.4 million of CSV was purchased using the av, sf, and za accounts in
14 over 400 transactions from devices using at least 34 different IP addresses beginning with
15 173.244.44, including IP addresses 173.244.44.19 (February 2018 and March 2018),
16 173.244.44.37 (December 2017 and March 2018), 173.244.44.58 (February 2018 and
17 March 2018), and 173.244.44.89 (January 2018, February 2018, and March 2018).
18 Microsoft investigators initially told me that they believed that the IP addresses beginning
19 in 173 were publicly-available IP address (such as one might find at a coffee shop with
20 WiFi) because other Microsoft employees had logged in via these addresses. As set forth
21 below, however, the investigation suggests that "173" IP addresses are not publicly
22 available.

23 36. The investigation has shown that KVASHUK used a 173.244.44.* IP
24 address to access a Microsoft store account linked to his personal email address,
25 kvashuk.volodymyr@gmail.com (the "kvashuk" account)⁷ at least nine times between
26 December 2 and December 19 of 2017, including IP addresses 173.244.44.19,
27

28 ⁷ The kvashuk.volodymyr@gmail.com account is listed as KVASHUK's personal account on his resume.

1 173.244.44.37, and 173.244.44.58. He also logged into his Coinbase cryptocurrency
 2 account using IP address 173.244.44.89 on December 2, 2017. However, no incidents
 3 have been identified where KVASHUK used a 173.244.44.* IP address and a test account
 4 used the same IP address on the same day to purchase CSV.

5 37. Records obtained through the course of the investigation indicate that IP
 6 addresses 173.244.44.19, 173.244.44.37, 173.244.44.58, and 173.244.44.89 are assigned
 7 to the company London Trust Media, Inc. This company operates a virtual private
 8 network⁸ (VPN) service that specializes in anonymity online under the name Private
 9 Internet Access through the website www.privateinternetaccess.com. The use of a VPN
 10 can effectively conceal the true IP addresses that somebody is using to connect to the
 11 Internet. While I am continuing to investigate the 173.244.44.* IP addresses, I believe
 12 that all of the 173.244.44.* IP addresses associated to this investigation are controlled by
 13 London Trust Media, Inc. Microsoft records show that Microsoft employees other than
 14 KVASHUK have logged in via the 173.244.44.* IP addresses. Based on my training and
 15 experience, and on information from other investigators, this does not suggest that the IP
 16 addresses are publicly available, but rather that other Microsoft employees have also used
 17 the London Trust VPN service.

18 38. Internet activity associated with the kvashuk.volodymyr@gmail.com
 19 account obtained from Google via a search warrant shows that KVASHUK conducted
 20 searches for terms related to, or visited websites for, Private Internet Access (or "PIA") at
 21 least once on November 27, 2017, and at least six times on December 17, 2017. The
 22 internet searches include the terms "pia hide tor traffic," "pia," "pia port forwarding," and
 23 "pia virus." Google records show he visited a Private Internet Access helpdesk article
 24 _____

25 ⁸ A virtual private network (VPN) is programming that creates a safe and encrypted connection over a less secure
 26 network, such as the public internet. A VPN works by using the shared public infrastructure while maintaining
 27 privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the
 28 sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data
 that is not properly encrypted. Often times, a VPN will also provide a proxy server service. With this service, a
 user's true IP address is masked when accessing resources on the internet, such as websites. The internet resource
 would only be able to see the IP address of the proxy server.

1 shortly after conducting these searches titled "Can I use TOR⁹ with the Private Internet
2 Access service." These searches suggest that, during the same time that the fraud scheme
3 was ramping up, KVASHUK was researching ways to conceal his identity on the
4 Internet.

5 39. According to records obtained from Microsoft, the first date a 173.244.44.*
6 IP address was used to obtain CSV as part of this scheme was on December 29, 2017,
7 when a CSV "purchase" was made through the av account. IP addresses in the
8 173.244.44.* range were used several times to obtain CSV through the av, sf, and za
9 accounts through March 23, 2018.

10 40. Based on my training and experience, and on information from other
11 investigators, KVASHUK may have believed that by using a VPN service specializing in
12 online anonymity to commit the fraud, he could disguise his involvement in the crimes.
13 Specifically, according to the Private Internet Access website, their VPN service provides
14 "IP Cloaking" by masking a user's IP address with one of their anonymous IP addresses.
15 Based on KVASHUK's experience as a software developer, and his experience working
16 with Microsoft on their online store, I believe he would know that the Microsoft online
17 store records the IP address of the users conducting transactions, and that a VPN service
18 would mask his true IP address, thereby disguising his involvement.

19 41. Another IP address, 4.35.246.19, was also used to access the av and sf test
20 accounts at least 24 times for purchases of over \$131,000 in CSV in connection with the
21 fraud. The IP address was also used to access three Microsoft store accounts linked to
22 KVASHUK. It was used at least 54 times between October 24, 2017 and November 24,
23 2017 to access the pikimajdo and xidijenizo accounts¹⁰ (the accounts used to order the
24

25 ⁹ In this context, TOR appears to be an acronym for "The Onion Router." TOR is an open-source software program
26 that allows users to disguise their IP address through encryption and by bouncing their internet traffic through
multiple other computers on the internet while operating compatible software.

27 ¹⁰ Federal Express tracking logs show a login to the company's tracking system in connection with an order placed
28 from the pikimajado email account. The login appears to be from Chesterbrook, PA. Although my investigation is
continuing, this login may have been done via a VPN, which allows the user to give the appearance of a login from a
different location than where the user is actually at.

1 graphics cards delivered to “Grigory Shikor” at KVASHUK’s apartment complex) and
2 used at least 21 times on November 24, 2017 to access the vokvas test account (the test
3 account created by KVASHUK). This IP address is registered to Level 3
4 Communications. By the time this IP address was provided to investigators, subscriber
5 records for the dates and times in question were outside of Level 3 Communications’
6 retention period.

7 42. A third IP address, 50.243.108.211, was used five times on December 12,
8 2017, to purchase approximately \$39,500 of CSV using the sf test account. It was also
9 used to access the vokvas account on June 5, 2017 and October 22, 2017, and the
10 xidijenizo account on October 22, 2017. The same IP address had also been used on
11 February 20, 2017 by KVASHUK when opening an account with the cryptocurrency
12 exchange Coinbase. As discussed below, KVASHUK deposited at least some of the
13 proceeds of the fraud into this Coinbase account. Level 3 Communications also provides
14 end user service for this IP address. By the time this IP address was provided to
15 investigators, subscriber records for the dates and times in question were outside of Level
16 3 Communications’ retention period.

17 43. The fact that all of the above IP addresses are linked to both KVASHUK
18 and the test accounts used to commit the fraud strongly suggests KVASHUK’s
19 involvement in the crime.

20 44. KVASHUK is also linked to the av and sf accounts through a technology
21 known as “Fuzzy Device” identification. When a person uses a particular device to
22 access Microsoft’s online store, that device leaves a digital trail known as a “Fuzzy
23 Device” identifier. According to Microsoft, although it is theoretically possible for two
24 devices to have the same Fuzzy Device ID, it is very unlikely. As a result, if multiple
25 logins are made from the same Fuzzy Device ID, there is a strong inference that the same
26 device (a particular computer, cell phone, etc.) was used to make all of those logins.

27 45. Between October 22, 2017, and November 26, 2017, Microsoft’s records
28 show the same Fuzzy Device ID for logins to accounts known or believed to be

1 associated with KVASHUK (the vokvas, xidijenizo, and pikimajado accounts) as well as
2 at least some logins to the accounts by which most of the CSV was stolen (av and sf).
3 Similarly, Microsoft records show that the user who logged into all of those accounts
4 was, on at least some occasions, running the same version of the Linux operating system
5 and the same outdated version of the Mozilla Firefox browser – further evidence that a
6 single device logged into all of those accounts.

7 46. The fuzzy device ID bb92c484-876b-4d87-adca-943b90a2d98e (the “98e”
8 ID) was the only fuzzy device ID used to make purchases on the Microsoft online store
9 by the accounts associated with the email addresses pikimajado@tinzoa.org and
10 xidijenizo@axsup.net. The 98e ID was also used to make purchases on the Microsoft
11 online store by the vokvas, av, and swfe2eauto accounts. According to Microsoft, no
12 other Microsoft store accounts were associated with the 98e ID.

13 47. Based on my training and experience, and on information from other
14 investigators, I know that the term “Device ID” is a generic industry term for an identifier
15 for an electronic device. Some devices have a unique identifier specifically labeled as a
16 “Device ID” by a hardware manufacturer. When one hardware manufacturer, website,
17 government agency, or any other company refers to the identification of, collection of, or
18 use of a “Device ID,” they are generally talking about a different identifier or mechanism
19 for generating a Device ID that is unique to that manufacturer or other entity. Device IDs
20 are generally used to identify multiple transactions conducted by the same device.

21 48. I also know that Device IDs are often created by collecting a very large
22 collection of not-so-unique browser and system components that a web-browser allows a
23 website to view/collect, such as operating system, web-browser, screen resolution, and
24 many other settings. If any of the settings used to calculate the Device ID change, the
25 Device ID will change. An individual with knowledge of Device IDs could disguise the
26 fact that they are conducting multiple transactions from the same device by changing
27 some of these settings. Additionally, Device IDs would change if the individual used
28

more than one device, or used virtual machines¹¹ to simulate the use of more than one device.

49. In total, Microsoft captured Fuzzy Device ID information on approximately 223 of the 1,554 purchases of CSV using the av, sf, and za accounts.¹² Over the course of the scheme, a total of 14 different Fuzzy Device IDs were captured on these 223 transactions. Most of the Fuzzy Device IDs were only used to purchase the CSV for one day. This could be indicative of using multiple devices, or the use of virtual machines. The first Fuzzy Device ID listed on the chart below – the 98e address – was used to access the vokvas, xidijenizo, and pikimajado accounts between October 22 and 24, 2017, and was also used to access the av and sf test accounts to make CSV purchases on November 26, 2017. This strongly suggests that the same device was used to access both accounts known to be linked to KVASHUK as well as the test accounts used to commit the fraud.

Device ID	Identified Purchase Transactions	Date Range
bb92c484-876b-4d87-adca- 943b90a2d98e	6	11/26/2017
58b04a06-d52c-481b-9050- 34d1f5c64aab	20	12/2/2017 – 12/13/2017
3bab2d39-29f9-4332-bc96- 3121a57d99cd	1	12/3/2017

¹¹ A virtual machine is simulated computer that runs its own operating system that runs like an application on another computer. The end user has a similar experience on a virtual machine as they would have if the operating system were installed on its own device. Several virtual machines can be installed on a single computer, and can be created in a short period of time. The use of a virtual machine could conceal the Device ID of the underlying device.

¹² Fuzzy Device ID information was only captured for transactions conducted through the av and sf accounts.

1	c2313cdc-a005-421b-9fa9-	3	12/7/2017
2	159d2adbdf53		
3	aa29eee2-3f6d-45b4-9c01-	11	12/9/2017
4	cfa320b962b1		12/12/2017
5	455010cd-e513-44c1-8fc0-	6	12/10/2017
6	f4495b0d7453		
7	6d2a6011-99b5-48be-b00c-	12	12/14/2017
8	130450b26272		
9	d117e690-0627-4624-912f-	19	12/15/2017
10	3a636457bf6d		
11	ec76885c-6718-4857-8cd9-	12	12/16/2017
12	8ea3f11ed30e		
13	84925e6b-035f-4138-9b41-	10	12/17/2017
14	b2dbbb13efce		
15	3b0d8c07-3656-4c4c-b938-	17	12/19/2017
16	8441c8c43716		12/20/2017
17	21c35123-ccef-474f-ade4-	79	12/22/2017
18	8fd96984975d		1/4/2018
19	486e5a23-b428-478c-99ed-	25	1/12/2018
20	7c25c8d76b25		
21	0424b94c-9e86-4abd-a9f4-	2	1/20/2018
22	bfce92f962a1		

Internet activity associated with the kvashuk.volodymyr@gmail.com account obtained from Google via a search warrant shows that KVASHUK searched for terms related to, or visited websites for or related to, "VM" or "virtualbox" (a virtual machine software) at least twenty times between November 7, 2017, and November 25, 2017.

Evidence of Unexplained Wealth

50. Financial records show that KVASHUK had a large amount of unexplained income during the period of the CSV thefts. According to his tax returns for 2016 and 2017, KVASHUK only had total income of \$35,260 and \$114,103, respectively. According to Microsoft, for the portion of time KVASHUK was a direct employee (December 2017 to June 2018), his annual salary was \$116,000.

51. Investigators have reviewed records for a checking account that KVASHUK had at Wells Fargo bank, ending in -5789. The earliest daily balance shown on the records was \$429.56 on July 29, 2016. The balance on the account remained under \$20,000 until late November of 2017, when large amounts of money from a cryptocurrency account in KVASHUK's name at Coinbase.com, began to flow into the -5789 account. On November 30, 2017, over \$14,000 was transferred to the -5789 account from Coinbase.com.¹³ On December 11, 2017, over \$6,600 was transferred from Coinbase.com to the -5789 account. On December 21, 2017, there was a transfer of over \$29,000 from Coinbase.com to the -5789 account.

52. The suspicious transfers escalated dramatically in early 2018. For example, on January 30th, February 2nd, and February 6th of 2018, there were transfers from Coinbase of over \$98,000, \$177,000 and \$134,000, respectively. On a single day – March 2, 2018 – over \$500,000 was transferred from Coinbase to the -5789 account. Over \$1.4 million was transferred in total in March 2018, followed by over \$935,000 in April.

53. All told, over \$2.8 million was transferred from Coinbase to the -5789 account between November 2017 and May 2018. The approximate timeframe of the vast majority of the fraud was November 2017 through March 2018. Given these timeframes, and based on my training and experience, it appears that KVASHUK had converted the

¹³ Of the \$14,876.98 transferred, \$5,024.01 was proceeds from the sale of Ethereum cryptocurrency. This cryptocurrency had been obtained in June 2017, and is not believed to be proceeds from the wire fraud scheme.

1 proceeds of the fraud into cryptocurrency (or received the proceeds as cryptocurrency),
2 and then gradually converted the cryptocurrency in fiat currency and transferred the
3 proceeds to his Wells Fargo account.

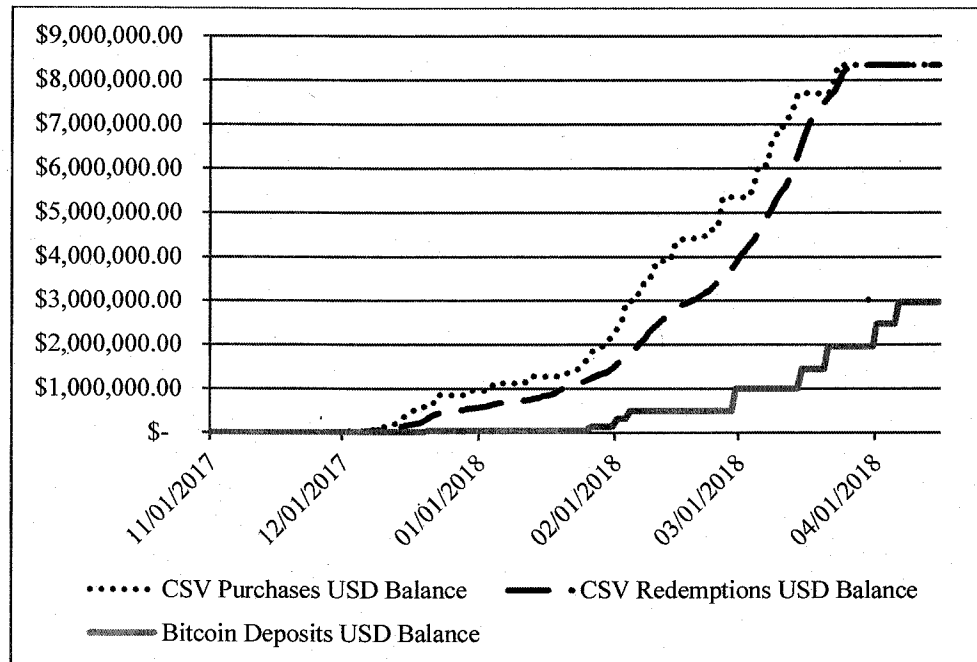
4 54. Furthermore, in order to determine the source of the cryptocurrency
5 “bitcoin” in the Coinbase account, SA Hergert has examined the bitcoin blockchain, a
6 public ledger of bitcoin transactions. SA Hergert determined that the vast majority of the
7 bitcoin deposited into the Coinbase account originated from chipmixer.com.
8 Chipmixer.com is a bitcoin “mixing” service which appears to be located in Germany. A
9 bitcoin mixing service mixes potentially identifiable bitcoin with others, with the intent to
10 obscure and conceal the original source of the bitcoin. Based on SA Hergert’s training
11 and experience, the use of chipmixer.com is further evidence of an attempt to conceal
12 proceeds of the fraud.

13 55. In addition to the bitcoin sourced from chipmixer.com, SA Hergert was
14 able to trace a deposit of 1.5 bitcoin into KVASHUK’s Coinbase account on November
15 29, 2017 from Paxful.com. Paxful.com is a peer-to-peer cryptocurrency trading site.
16 This site allows users to purchase bitcoin with gift cards, including Xbox gift cards.
17 Internet activity associated with the kvashuk.volodymyr@gmail.com account obtained
18 from Google via a search warrant showed KVASHUK searched for terms related to, or
19 visited websites for or related to, paxful.com at least three times between November 24,
20 2017 and November 27, 2017. This is further evidence of KVASHUK researching
21 matters relevant to the fraud at the approximate time that the fraud scheme ramped up
22 dramatically.

23 56. As part of the investigation, SA Hergert analyzed the value of bitcoin (in
24 United States dollars) deposited into KVASHUK’s Coinbase account and compared it to
25 the purchases and redemptions of CSV.¹⁴ SA Hergert was able to determine that, while
26 significantly lower, the value of the bitcoin deposits to KVASHUK’s Coinbase account
27

28 ¹⁴ This analysis does not take into account the value of any CSV that was blacklisted by Microsoft.

generally correlated with the value of the purchased and redeemed CSV. The reasons for the lower value could include KVASHUK selling the CSV at a discount, bitcoin's general decline in value during early 2018, or that not all of the proceeds from this scheme have been identified.



57. KVASHUK has used his unexplained wealth to make significant purchases. In March of 2018, KVASHUK paid roughly \$162,000 for a Tesla vehicle. According to title company records, in June of 2018, KVASHUK bought a lakeside home in Renton for roughly \$1.675 million.

58. KVASHUK told Microsoft investigator Andrew Cookson, in an interview on May 16, 2018, that he had rented a new place since the last time they spoke. In truth, records obtained during that investigation show that he had accepted a purchase agreement for the Renton home as of approximately April 1, 2018, and a rental agreement to occupy the property prior to closing dated April 19, 2018. Email messages from Amazon.com to KVASHUK show purchases of items to be delivered to him at the Renton home as early as April 24, 2018.

1 *False Tax Returns*

2 59. On or about February 24, 2018, KVASHUK electronically filed a 2017
3 Form 1040, *U.S. Individual Income Tax Return*, with the IRS. The tax return appears to
4 have been self-prepared by KVASHUK using the website 1040.com. The tax return
5 reported income of \$109,440 from wages, and net gains of \$4,663 from the sale of
6 various cryptocurrencies, including bitcoin, for total reported income of \$114,103.
7 Deposits into KVASHUK's Wells Fargo bank account *5789 in 2017 totaled
8 \$139,680.76.

9 60. On or about February 21, 2019, a 2018 Form 1040, *U.S. Individual Income*
10 *Tax Return*, was filed electronically for KVASHUK by Tax Rite, Inc. The tax return was
11 prepared by a paid return preparer. The tax return reported income of \$76,927 from
12 wages, \$9,968 from dividends, and a loss of \$71,745 (limited to a deductible loss of
13 \$3,000) from the sale of investments and cryptocurrency, including bitcoin, for total
14 reported income of \$83,895. Deposits into KVASHUK's Wells Fargo bank account
15 *5789 in 2018 totaled \$2,925,374.48.

16 61. As shown above, KVASHUK, through his scheme to defraud Microsoft,
17 acquired CSV totaling approximately \$971,161.26 in 2017 and \$7,385,730.04 in 2018 at
18 no cost to himself. These amounts are includable in his gross income, and are taxable in
19 the year they are received.

20 62. KVASHUK did report the income from the sales of bitcoin to Coinbase
21 discussed above. However, in 2017 he only reported a taxable gain (sales price less
22 basis) of approximately \$1,547 in 2017 and a loss of approximately \$69,418 in 2018.
23 The limited gain and the loss reported on the tax returns appear to be the result of
24 KVASHUK using the value of the bitcoin at the time he deposited them into his Coinbase
25 account as his basis. In truth, because the bitcoin were obtained as proceeds of his
26 scheme to defraud, and since KVASHUK did not report the income from his scheme to
27 defraud, his basis in the bitcoin should have been \$0. If this were the case, he would
28 have had income from the sale of bitcoin obtained through the scheme of \$47,715 in 2017

1 and \$2,846,041 in 2018, based on the sales proceeds reported on his respective tax
2 returns.

3 63. On December 19, 2017, KVASHUK emailed J.P. from taxhotline.net.
4 Based on the context of the email, it appears to be a follow-up discussion to a prior phone
5 call. In the message, KVASHUK indicated he was receiving gifts from his father in the
6 form of bitcoin and questioned how to show on a tax return that the funds were a gift so
7 he wouldn't "have any troubles in the future." He specifically noted that his father
8 purchased the bitcoin with cash, and therefore had no records of the purchase.

9 64. On February 5, 2019, KVASHUK emailed D.L., his tax return preparer,
10 regarding the preparation of KVASHUK's 2018 tax return. In the email, he told D.L.
11 that his father sent him bitcoin, which he sold to Coinbase for cash, and references a
12 computer file that appears to be a report from Coinbase regarding transactions conducted
13 in his Coinbase account. Based on SA Hergert's review of the tax return, the proceeds
14 from bitcoin sales reported on the tax return reconcile to the U.S. currency withdrawn
15 from Coinbase, and the cost basis claimed materially reconciles to the U.S. dollar value
16 recorded by Coinbase at the time the bitcoin was deposited to KVASHUK's account.


17 65. As discussed above, while conducting blockchain analysis on the bitcoin
18 deposited into KVASHUK's Coinbase account, SA Hergert was able to determine that
19 the majority of the bitcoin appeared to trace back to Paxful.com and Chipmixer.com.

20 66. Additionally, an email between KVASHUK and his father on May 18,
21 2018 includes copies of a 2018 non-immigrant visa application for KVASHUK's father
22 which stated his father was a university lecturer with a monthly income of 30,000 in
23 Ukrainian currency. Based on the exchange rate on that day, this would be approximately
24 \$1,156 per month.

25 //

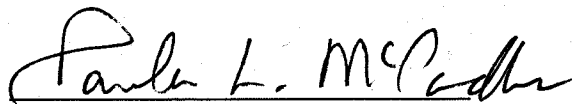
26 //

1 67. Based on the above facts, I respectfully submit that there is probable cause
2 to believe that VOLODYMYR KVASHUK committed the crime charged in Count 1,
3 above.

4
5 
6 MICHAEL SPIESS, Complainant
7 Special Agent
8 United States Secret Service

9 Based on the Complaint and Affidavit sworn to before me, and subscribed in my
10 presence, the Court hereby finds that there is probable cause to believe the Defendant
11 committed the offense set forth in the Complaint.

12 Dated this 16th day of July, 2019.

13
14 
15 PAULA L. MCCANDLIS
16 United States Magistrate Judge
17
18
19
20
21
22
23
24
25
26
27
28